CLAIMS

1. A security device comprising at least one magnetic element, wherein said at least one magnetic element is responsive to an applied magnetic field to provide a characteristic response, characterised in that said at least one magnetic element is made from a material that comprises structural defects that cause brittle mode switching in which the growth of a single magnetic domain dominates the change in magnetisation of a respective magnetic element.

2. The security device of Claim 1, wherein said at least one magnetic element is supported by a substrate.

3. The security device of Claim 2, wherein said at least one magnetic element is supported on said substrate.

4. The security device of any preceding Claim, wherein said at least one magnetic element is responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of said at least one magnetic element.

5. The security device of any preceding Claim, wherein said at least one magnetic element is made from a magnetically soft material.

6. The security device of Claim 5, wherein said at least one magnetic element comprises a magnetically soft material selected from one or more of: nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.

7. The security device of Claim 5 or 6, wherein said magnetically soft material is a permalloy material.

8. The security device of any preceding Claim, wherein said at least one magnetic element is substantially wire-shaped or flattened wire shaped.

9. The security device of any preceding Claim, wherein said at least one magnetic element is backed by a light reflective layer.

10. The security device of any preceding Claim, wherein said at least one magnetic element is provided proximal a reduced light reflectivity portion of said security device.

11. The security device of any preceding Claim, comprising a plurality of said at least one magnetic elements.

12. The security device of Claim 11, wherein said plurality of magnetic elements is arranged to provide a linear pattern.

13. The security device of Claim 11, wherein said plurality of magnetic elements is arranged to provide a two-dimensional pattern.

14. The security device of Claim 12 or Claim 13, wherein said pattern encodes an identifier.

15. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.

16. The security device of claim 15, wherein said unique identifier is provided by way of one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

17. The security device of claim 16, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.

18. The security device of any preceding Claim, wherein premeasured characteristic response information representing one or more measurable parameters of said characteristic response is stored on said security device.

19. The security device of Claim 18, wherein said premeasured characteristic response information is in encrypted form.

20. A method of manufacturing a security device, comprising:

providing at least one magnetic element comprising structural defects, wherein said at least one magnetic element provides a brittle mode switching characteristic response in response to an applied magnetic field.

21. The method of Claim 19, comprising providing said at least one magnetic element on a substrate.

22. The method of Claim 20 or Claim 21, comprising forming said at least one magnetic element using a lift-off or wet etching process.

23. The method of Claim 20 or Claim 21, comprising forming said at least one magnetic element using an ion beam etching process.

24. The method of any one of Claims 20 to 23, comprising measuring the magnitude(s) of one or more magnetic parameters of said at least one magnetic element.

25. The method of Claim 24, comprising measuring one or more of coercivity and jitter values.

26. The method of Claim 24 or Claim 25, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.

27. The method of Claim 26, comprising encrypting said premeasured characteristic response information.

28. The method of Claim 26 or Claim 27, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.

29. The method of Claim 26 or Claim 27, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.

30. The method of Claim 29, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.

31. The method of any one of Claims 20 to 30, further comprising providing said security device with a unique identifier.

32. The method of Claim 31 when dependant upon any one of Claims 27 to 30, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.

33. A system for reading a security device, comprising:

a magnetic field generation system for applying a magnetic field to a security device; and

a detection system for measuring one or more parameters representative of a brittle mode switching measured characteristic response of said security device in response to said magnetic field,

wherein said system is operable to compare said one or more parameters representative of a brittle mode switching measured characteristic response to one or more respective parameters of a brittle mode switching premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

34. The system of Claim 33, wherein the magnetic field generation system is operable to apply a time varying magnetic field to a security device.

35. The system of Claim 33 or Claim 34, wherein a light beam is used to interrogate said security device.

36. The system of any one of Claims 33 to 35, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

37. The system of any one of Claims 33 to 36, wherein said parameters represent one or more of coercivity and jitter values.

38. The system of any one of Claims 35 to 37, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for detecting changes induced in said light beam by magnetic elements of said security device.

39. The system of Claim 38, wherein said magneto-optic Kerr effect detection apparatus is configured to operate in transverse mode.

40. The system of any one of Claims 35 to 39, further operable to deflect said light beam across the surface of said security device.

41. The system of any one of Claims 33 to 40, further operable to read a unique identifier from said security device.

42. The system of Claim 41, wherein said unique identifier is identified by recognising a pattern of magnetic elements supported by said security device.

43. The system of Claim 41 or 42, wherein said unique identifier is identified by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

44. The system of any one of Claims 33 to 43, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

45. The system of any one of Claims 33 to 44, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

46. The system of Claim 45, wherein said database is remotely located from said detection system.

47. The system of any one of Claims 33 to 46, further operable to decrypt premeasured characteristic response information where it is read or provided in encrypted form.

48. A method for reading a security device, comprising:

applying a magnetic field to a security device;

measuring one or more parameters representative of a brittle mode switching measured characteristic response of said security device in response to said magnetic field; and

comparing said one or more parameters representative of a brittle mode switching measured characteristic response to one or more respective parameter(s) of a brittle mode switching premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

49. The method of Claim 48, comprising applying a time varying magnetic field to a security device.

50. The method of Claim 48 or Claim 49, wherein measuring of one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field comprises measuring one or more of coercivity and jitter values.

51. The method of any one of Claims 48 to 50, comprising interrogating said security device using a light beam.

52. The method of any one of Claims 48 to 51, comprising operating a laser to produce a visible or near-infrared beam.

53. The method of Claim 51 or Claim 52, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.

54. The method of Claim 53, comprising using the magneto-optic Kerr effect transverse mode.

55. The method of any one of Claims 51 to 54, comprising deflecting said light beam across the surface of said security device.

56. The method of any one of Claims 48 to 55, comprising reading a unique identifier from said security device.

57. The method of Claim 56, comprising identifying said unique identifier by recognising a pattern of magnetic elements supported by said security device.

58. The method of Claim 56 or 57, comprising identifying said unique identifier by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

59. The method of any one of Claims 48 to 58, comprising determining said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

60. The method of any one of Claims 48 to 59, comprising determining said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

61. The method of Claim 60, comprising accessing a database remotely located from said detection system.

62. The method of any one of Claims 48 to 61, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.

63. A product comprising the security device of any one of Claims 1 to 19.

64. The product of Claim 63, comprising one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging; an item of clothing; an item of footwear; a smart-card; a credit or bank card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.